New Jersey Department of Children and Families Policy Manual

Manual:	OOE	Office of Education	Effective Date:
Volume:	I	Office of Education	
Chapter:	A	Office of Education	6-11-2012 rev. 10-15-2013
Subchapter:	1	Office of Education	
Issuance:	54	**Internet Safety**	Revised:

SUBJECT: Internet Safety

EFFECTIVE DATE: June 11, 2012

A. OBJECTIVE:

To provide a policy and guidelines for Department of Children and Families (DCF) Regional Schools which specify appropriate use of computers and the Internet by students and to certify compliance with the Children's Internet Protection Act (CIPA) of December 21, 2000 and the Protecting Children in the 21st Century Act.

B. DEFINITIONS:

Blog: a blog is a personal journal published on the Internet, consisting of discrete entries ("posts") typically displayed in reverse chronological order so the most recent post appears first. Blogs may be the work of a single individual or a small group, and often are themed on a single subject. In an educational context, a blog may serve as an informational form of expression, debate, opinion, etc. for various student-centered projects.

Chat Room: The term chat room is any form of synchronous conferencing (typing in text and receiving responses back in a text format). The term can therefore mean any technology ranging from real-time online chat utilizing instant messaging and online forums around topics of interest to that user group. The primary use of a chat room is to share information via text with a group of other users. Thus, the ability to converse with multiple people in the same conversation differentiates chat rooms from instant messaging programs, which are more typically designed for one-to-one communication.

Cyber-bullying: Cyber-bullying is the repeated or single incident use of information technology; including the Internet, e-mail, instant messaging, text messages, blogs, chat

rooms, social networking sites (e.g. Facebook, Twitter, etc.) pagers, cell phones and gaming systems to deliberately harass, threaten, harm or intimidate others. Unlike physical bullying, where the victim can walk away, technology allows for continuous, and often anonymous, harassment, from any distance, in a variety of ways.

Hacking: any method to gain unauthorized access to a computer or a network system which may or may not result in interfering with or sabotaging that computer/network system or which may be motivated by maliciousness or attempts at personal gain.

Inappropriate Matter: Visual depictions which are obscene, pornographic (child or adult-related); text material which describes hate crime-related topics or any other violent/abusive/racist/sexist matter; and other prohibited areas as determined and communicated periodically by the Director, DCF Office of Education (OOE).

Social Networking Sites: Social networking sites focus on building relationships among people who share interests and/or activities. A social network may include the name and other representations of each user (in the form of a "profile"), his or her social links and a variety of additional information. Most social networking is Internet-based and allows users to interact over the Internet through e-mail and instant-messaging. Social networks allow users to share ideas, activities, events, interests within their individual networks.

Technology Protection Measure: A technology protection measure is a specific technology that blocks or filters Internet access. It protects against access by adults and students, whether an adult student or a minor-aged student, to visual depictions that are obscene, child pornography, or otherwise harmful.

Wiki: a wiki is a website in which users can add, modify, or delete content. In an educational context, a wiki may serve as an informational hub for various student-centered projects.

C. STANDARDS:

1. Educational staff shall monitor the online activities of students whenever a student accesses the Internet.

2. Access to inappropriate matter on the Internet by school personnel and all students, whether an adult student or a minor-aged student, is prohibited and shall be vigilantly monitored by educational staff.

3. The safety and security of all students when using permitted electronic mail, chat rooms, and other forms of direct electronic communications, shall be monitored by educational staff.

4. Unauthorized access, including "hacking" and other unlawful activities, by any student using the Internet is prohibited and shall be vigilantly monitored by educational staff.

5. Unauthorized disclosure, use, and dissemination of personal student information in any print or electronic format is prohibited and shall be vigilantly monitored by educational staff.

6. Technology Protection Measures designed to restrict students' access to harmful materials shall be continuously upgraded, installed and monitored for efficacy by educational staff with the support of the Education Technology Unit (ETU) at the DCF Office of Education (OOE).

7. The disabling of any blocking or filtering system is prohibited unless expressly approved in writing by the Director, OOE.

D. PROCEDURES:

1. The specific technology that blocks or filters Internet access, including inappropriate matter and images as defined in the Technology Protection Measure and the Inappropriate Matter definitions above is the "Websence" system.

    a. This filtering system shall be installed on the mainframe servers which then manages and protects all computers with Internet access in each DCF Regional School building.

    b. The "Websence" product may, upon the direction of the DCF administration, periodically be replaced by other, similar and upgraded products.

    c. The "Websence" filter system protects against access by adults and minors to visual depictions that are obscene, child pornographic or harmful to minors by filtering key words. Additionally, this system is designed to provide state-of-the-art security to the users of the Internet and DCF network. It consists of multiple firewalls with strict firewall rules protecting the network resources from abuse.

2. When permitted and approved by the Director, OOE, student use of electronic mail, chat rooms, wikis, blogs, social networking sites and other forms of direct electronic communications shall be vigilantly monitored by educational staff.

    a. Prior to any pre-approved student use of electronic mail, chat rooms, social networking sites and other forms of direct electronic communications, a series of instructional lessons regarding online safety shall be provided to the students within each OOE Regional School. These lessons shall facilitate the

students' understanding of social networks and chat rooms and specifically instruct students in the inherent risks and negative consequences that can result from their inappropriate use of these forms of communication.

b. The use of these forms of electronic communication shall be noted in a teacher's lesson plan and approved by the ES prior to implementation of the instructional experience.

c. The classroom teachers shall supervise and monitor students while using these forms of electronic communication.

d. With the exception of permitted student use of electronic mail, chat rooms and other electronic communications, any inappropriate communication observed on a computer shall be subject to the following actions:

    1) The teacher shall immediately remove the student from the computer area;
    2) The teacher shall call for the ES to witness the image/material on the computer;
    3) The ES shall make a note of the inappropriate material;
    4) The ES shall contact the ETU at the OOE;
    5) The ETU shall re-verify the filtering process and take action as appropriate;
    6) The ES shall subsequently delete the inappropriate material.

e. The ES shall apply the appropriate disciplinary sanctions against the student in accordance with the Code of Student Conduct.

3. Unauthorized computer access including "hacking" as defined above and other unlawful activities by any student using the Internet is prohibited and shall be vigilantly monitored by educational staff.

    a. If any inappropriate "hacking" activity is observed on a computer:

        1) The teacher shall immediately remove the student from the computer area;
        2) The teacher shall call for the ES to witness the material on the computer;
        3) The ES shall make a note of the inappropriate material;
        4) The ES shall contact the ETU at the OOE;
        5) The ETU shall re-verify the filtering process and take action as appropriate;
        6) The ES shall subsequently delete the inappropriate material.

    b. The ES shall apply the appropriate disciplinary sanctions against the student in accordance with the Code of Student Conduct.

4. Unauthorized disclosure, use and dissemination of personal student information in any print or electronic format is prohibited and shall be vigilantly monitored by educational staff.

    a. Students who have been victimized by having their personal information revealed or shared in an unauthorized manner shall report such incident(s) to the ES.

    b. The ES shall, upon discovery of the illicit or intentional personal information sharing, make a record of the information that was shared publicly and subsequently take all reasonable steps to delete the information about the student.

    c. If a student was discovered to have posted or shared his/her own personal information in an unauthorized manner, the appropriate disciplinary measures shall be applied by the ES in accordance with the Code of Student Conduct.

    d. If a student was discovered to have posted or shared personal information about another student, the ES shall apply the appropriate disciplinary measures against the guilty student in accordance with the Code of Student Conduct.

5. Authorized disclosure, use and dissemination of students' personal information on a computer may be permitted when approved by the Director, OOE. If approved, this limited personal information sharing may be for use in a student's "electronic portfolio" or other, similar approved projects.

6. Cyber-bullying awareness and response shall be the responsibility of all educational staff and students within each DCF Regional School and shall include the following measures:

    a. Instruction on cyber-bullying awareness and the school's responses shall be provided to students.

    b. Any incident or suspected incident of cyber-bullying shall immediately be reported to the ES.

    c. The ES shall, whenever possible, make a record of the incident by noting exactly the text or other media form that constitutes the cyber- bullying.

    d. As feasible, the ES shall document the source of the Cyber-bullying incident.
    e. If any aspect of this Internet Safety Policy and/or the "Harassment, Intimidation and Bullying" (OOE Policy # 53) has been violated by a student, the ES shall apply the appropriate disciplinary measures in accordance with the Code of Student Conduct.

f. The ES shall complete an Unusual Incident Report, in accordance with OOE Policy # 29.

g. The ES shall also report to law enforcement authorities any Cyber- bullying incident which is a violation of State or Federal law.

7. For any student violation of any of the above prohibited activities, the ES shall additionally notify the Regional Administrator of the infraction and the disciplinary actions applied.

8. For any employee, contracted service provider, intern, visitor or volunteer found to have violated any of the above prohibited activities, the ES shall notify the Regional Administrator and apply the following actions:

   a. The consequences for an employee shall be applied in accordance with the appropriate corrective actions and disciplinary measures as directed by the applicable Office of Cooperative Labor Relations and Office of Equal Employment Opportunity/ Affirmative Action (EEO/AA).

   b. The consequences for a contracted service provider shall be applied in accordance with the policies of the vendor, and may be grounds for termination of the existing contract, depending upon the nature and severity of the violation. Referral to the Office of Equal Employment Opportunity/Affirmative Action (EEO/AA) will be made, as appropriate.

   c. The consequences and appropriate remedial action for an intern, visitor or volunteer shall be determined after consideration of the nature, severity and circumstances of the act, including law enforcement reports or other legal actions, and may include termination of the internship, removal of building or grounds privileges, prohibiting contact with students and/or prohibiting the provision of student services.

E. TRAINING AND UPDATES:

1. All OOE and Regional School staff, contracted service providers, interns, volunteer providers or any other long-term service provider (paid or unpaid) shall receive training on this policy as follows:

   - Upon initial publication of the policy;
   - Upon initial employment;
   - Upon initial provision of services by interns, volunteers or long-term service providers; and
   - When policy updates or revisions are issued.

2. Students in DCF Regional Schools shall be trained on the relevant aspects of this policy as identified in the “Definitions” and “Procedures” sections.

3. DCF shall have the authority to periodically update and revise the technology, filtering system and other aspects related to computer and internet security.

_____
Tracy Nowlin